REMARKS

Claim Amendments

Applicants have amended independent claims 39 and 57 to incorporate features recited in dependent claims 40 and 58, and accordingly, canceled claims 40 and 58 without prejudice or disclaimer of their subject matter. Support for the amendments to independent claims 39 and 57 can also be found in the specification at, for example, p. 6, lines 31-33, and p. 7, lines 5-8. In addition, Applicants have amended claims 74 and 77. Support for the amendments to claim 77 can be found in the specification at, for example, p. 5, lines 4-7. No new matter has been introduced. Upon entry of this Amendment, claims 39, 41-57, and 59-77 remain pending.

Office Action

In the Office Action, the Examiner took the following actions:

(a) objected to the specification;

(b) rejected claims 57-76 under 35 U.S.C. § 101;

(c) rejected claims 39-43, 56-62, and 75-77 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,716,742 ("Roesch");

(d) rejected claims 44 and 63 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of U.S. Patent No. 7,305,708 ("Norton");

(e) rejected claims 45-47, 50-53, 64-66, and 69-72 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of an article titled "Intrusion detection system for high-speed network" ("Yang");

(f) rejected claims 48, 49, 67, and 68 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Yang, and further in view of U.S. Patent No. 7,620,988 ("Hernacki");

(g) rejected claims 54, 55, and 73 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Yang, and further in view of U.S. Patent No. 7,660,248 ("Duffield"); and

(h) rejected claim 74 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Duffield.

Objection to the Specification

The Office Action objected to the specification "because it contains an embedded hyperlink and/or other form of browser-executable code." Office Action, p. 2. In response, Applicants have amended the specification to delete the hyperlink from p. 12, line 26. Applicants therefore respectfully request withdrawal of the objection.

Rejection of Claims 57-76 under 35 U.S.C. § 101

The Office Action rejected claims 57-76 under 35 U.S.C. § 101, alleging that "the claims are directed to a system including modules, which could be directed to software, per se. The software embodiment does not fall within one of the statutory classes of invention defined under 35 U.S.C. §101." Office Action, p. 2.

Without conceding to the Office Action's allegations, and for the sole purpose of advancing prosecution, Applicants have amended claim 57 as indicated herein. Applicants therefore respectfully request withdrawal of the rejection.

Rejection of Claims 39-43, 56-62, and 75-77 under 35 U.S.C. § 102(e)

The rejection of claims 40 and 58 has been rendered moot by virtue of their cancellation. Applicants respectfully traverse the rejection of claims 39, 41-43, 56, 57, 59-62, and 75-77 under 35 U.S.C. § 102(e) as being anticipated by Roesch. *See* Office Action, pp. 3-4. In order to establish anticipation under 35 U.S.C. § 102, the Office Action must show that each and every feature as set forth in the claim is found, either expressly or inherently described, in Roesch. *See* M.P.E.P. § 2131.

First, Roesch *may not* constitute prior art under 35 U.S.C. § 102(e) against the present application. Applicants note that Roesch was filed on May 12, 2004, which is *later* than the March 30, 2004 PCT filing date of the present application. Roesch claims priority to U.S. Provisional Application No. 60/469,395 ("Roesch '395"), filed on May 12, 2003, which is *earlier* than the PCT filing date of the present application. However, because Roesch contains additional subject matter not present in Roesch '395, Roesch would not necessarily be entitled to the benefit of the Roesch '395 provisional filing date. Therefore, if the portions of Roesch relied upon by Office Action were not originally disclosed in Roesch '395, Roesch should not be entitled to a priority date of May 12, 2003. The Office has not shown that Roesch would be entitled to the priority date of its provisional application, and therefore cannot apply Roesch as prior art under 35 U.S.C. § 102(e) against the present application.

Second, Roesch '395 discloses "a system and method for automatically and passively determining a host configuration of a computer network." Roesch '395, ¶ [0001]. Specifically, Roesch '395 discloses "obtain[ing] the operating system of a host machine using IP fingerprinting." *Id.*, ¶ [0019]. "[W]hen a packet is detected moving through the network[, t]he packet is parsed for TCP protocol flags . . . [that] are used to determine if the packet is from a server or client computer." *Id.* Then "[t]he origin of the packet is used to select a fingerprinting tree data structure" (*id.*), which "uniquely associates operating systems with one or more packet fields." *Id.*, ¶ [0020]. Roesch '395 discloses that "a 'fingerprint' includes the window size, maximum segment size, DF bit, window scale, SACKOK bit, NOP flag, packet size and time to live fields of a packet." *Id.*, ¶ [0021].

In rejecting claim 39, the Office Action cites to Roesch's col. 15, lines 1-20, for its disclosure of "detect[ing] operating systems [and] services." Office Action, p. 3. Applicants note that Roesch's col. 15, lines 1-20 discusses Fig. 9, which is different from Fig. 6 originally disclosed in Roesch '395. For example, the "protocol field analyzer 940" depicted in Fig. 9 of Roesch was not originally disclosed in Fig. 6 of Roesch '395. Although Fig. 6 of Roesch '395 discloses a "fingerprint tree analyzer," it does not provide support for the "protocol field analyzer 940" depicted in Fig. 9 of Roesch. Applicants note that the descriptions of the "fingerprint tree analyzer" in the original specification of Roesch '395 do not include any description of "protocol field," "protocol field" analysis, or "protocol field analyzer." *See* Roesch '395, ¶¶ [0029]-[0030]. Furthermore, the "application fingerprint table 955" depicted in Fig. 9 and discussed at col. 15, lines 1-20 of Roesch is completely missing from the disclosure of Roesch '395. Therefore, the Office Action's reliance on Roesch's col. 15, lines 1-20 *cannot* be applied as prior art because Roesch is not entitled to the benefit of the Roesch '395 provisional filing date for this subject matter.

Regardless of whether the specific portions of Roesch cited by the Office Action are entitled to the filing date of May 12, 2003 of Roesch '395, the Office Action can only rely on information in Roesch that was originally disclosed in, and supported by, Roesch '395. As discussed above, Roesch '395 discloses determining "the operating system of a host machine using IP fingerprinting." Roesch '395, ¶ [0019]. Roesch '395 also discloses that "services being run on servers are identified using TCP/IP ports." *Id.*, ¶ [0025].

Roesch '395, however, does not disclose or suggest "application layer protocols," as recited in independent claim 39 (Applicants note that the "application protocol" disclosed at col. 13, lines 7-8 of Roesch was not originally disclosed in Roesch '395). In addition, determining the "operating system" of a host machine, as disclosed in Roesch '395, is completely different from "detecting information relating to application layer protocols associated with said monitored data flows independently of said network ports," as recited in claim 39, at least because the "operating system" of a host machine is not an "application layer protocol[]," as one of ordinary skill in the art could appreciate. According to Roesch '395, the term "operating system" refers to operating systems such as "OS X," "FreeBSD," "Linux," "Irix", and "Windows." *See e.g.*, Fig. 5 of Roesch '395. In contrast, an "application layer protocol[]," as recited in claim 39, refers to application layer protocols such as "ftp(21)" and "http(80)." *See e.g.*, Specification of the present application, p. 15, line 12 to p. 16, line 14. Thus, the mere disclosure of detecting operating systems by Roesch '395 does not constitute a disclosure of "detecting information relating to application layer protocols," as recited in claim 39.

The Office Action also alleges that Roesch discloses "detect[ing] . . . services." Office Action, p. 3. First, "services" are not "application layer protocols," as recited in claim 39. Second, even assuming, solely for the sake of argument, that "application layer protocols" read on Roesch's "services," Roesch '395 discloses that "services being run on servers are identified using TCP/IP ports." Roesch '395, ¶ [0025] (emphasis added). This is contrary to "detecting information relating to application layer protocols associated with said monitored data flows independently of said network ports," as recited in amended claim 39 (emphasis added).

Moreover, for at least the same reasons discussed above, Roesch also does not disclose or suggest "providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols independently of any predefined association between said network ports and said application layer protocols," as recited in amended claim 39 (emphasis added).

Therefore, Roesch does not disclose or suggest each and every feature of amended claim 39. Accordingly, claim 39 should be allowable over Roesch. Although of different scope, amended independent claim 57 recites features similar to those discussed above in connection with amended claim 39. Therefore, claim 57 should also be allowable over Roesch for at least the same reasons discussed above with respect to claim 39. In addition, dependent claims 41-43, 56, 59-62, and 75-77 should be allowable over Roesch at least by virtue of their respective dependence from base claim 39 or 57, and because they recite additional features not disclosed in Roesch. Applicants therefore respectfully request withdrawal of the rejection.

Rejection of Claims 44 and 63 under 35 U.S.C. § 103(a)

Applicants respectfully traverse the rejection of claims 44 and 63 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Norton. *See* Office Action, p. 4.

As discussed above, Roesch does not teach or suggest the claimed steps of "detecting" and "providing," as recited amended independent claim 39 (and similarly recited in amended independent claim 57). Norton does not cure the deficiencies of Roesch.

Norton discloses enhancing the performance of an intrusion detection system "with the addition of rule optimization, set-based rule inspection, and protocol flow analysis." Norton, Abstract. Although Norton discloses determining the protocol (such as HTTP) associated with the packet, for example, at step 920 of Fig. 9 (*see also*, col. 16, lines 65-67), Norton's rules for intrusion detection are provided based on network ports. For example, Norton discloses that "[o]ne exemplary IDS created rule sets [was] based on four parameters. These were source IP address, destination IP address, source port range, and destination port range." *Id.*, col. 7, lines 11-13. Norton also discloses that "a TCP rule may be unique from other TCP rules based on the source and destination ports." *Id.*, col. 7, lines 59-61 (emphasis added).

Further, Norton's intrusion detection appears to be provided by utilizing the relationship or association between the network ports and the application layer protocols. For example, Norton discloses at col. 8, lines 48-60, that

> . . . HTTP client request traffic needs to be inspected against HTTP client request rules, not HTTP server response rules. So when a packet is coming from the HTTP client, which means that "port 80" is in the TCP destination port field, both the source and destination ports are checked for unique ports. Almost always for client HTTP traffic, the source port is not a unique port, because it is above 1024, but the destination port is since it is destined to an HTTP server, which usually resides on port 80 or another defined HTTP server port. So in the case of an HTTP client packet, the rule set with the parameters of "destination port 80" and "source

> port generic" is selected, and gets inspected by detection engine 240.

For at least these reasons, Norton *teaches away* from "providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols independently of any predefined association between said network ports and said application layer protocols," as recited in amended claim 39 (and similarly recited in amended independent claim 57) (emphasis added).

Roesch and Norton, therefore, whether taken alone or in combination, do not teach or suggest each and every feature of independent claims 39 and 57. Accordingly, claims 39 and 57 should be allowable over Roesch and Norton. Dependent claims 44 and 63 should also be allowable over Roesch and Norton at least by virtue of their respective dependence from base claim 39 or 57, and because they recite additional features not taught or suggested in Roesch and Norton. Applicants therefore respectfully request withdrawal of the rejection.

Rejection of Claims 45-47, 50-53, 64-66, and 69-72 under 35 U.S.C. § 103(a)

Applicants respectfully traverse the rejection of claims 45-47, 50-53, 64-66, and 69-72 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Yang. *See* Office Action, pp. 5-7. As discussed above, Roesch does not teach or suggest the claimed "detecting" and "providing" steps, as recited in amended independent claim 39 (similarly recited in amended independent claim 57). Yang does not cure the deficiencies of Roesch.

Yang discloses an "intrusion detection system for high-speed network." Yang, Title. Yang's system includes a rule-based detection engine. *See* Yang, § 3.4, p. 1292. Yang's rule "consists of a rule head and rule options. The rule head includes source IP . . . , destination IP (192.168.1.0/24), source port (any), destination port (111), [and] protocol type (tcp) . . . ." *Id.* Thus, Yang's rule for intrusion detection is provided based on both the protocol and the network ports. Accordingly, Yang *teaches away* from "providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols independently of any predefined association between said network ports and said application layer protocols," as recited in amended claim 39 (and similarly recited in amended independent claim 57) (emphasis added).

Roesch and Yang, therefore, whether taken alone or in combination, do not teach or suggest each and every feature of independent claims 39 and 57. Accordingly, claims 39 and 57 should be allowable over Roesch and Yang. Dependent claims 45-47, 50-53, 64-66, and 69-72 should also be allowable over Roesch and Yang at least by virtue of their respective dependence from base claim 39 or 57, and because they recite additional features not taught or suggested in Roesch and Yang. Applicants therefore respectfully request withdrawal of the rejection.

Rejection of Claims 48, 49, 67, and 68 under 35 U.S.C. § 103(a)

Applicants respectfully traverse the rejection of claims 48, 49, 67, and 68 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Yang, and further in view of Hernacki. *See* Office Action, pp. 7-8.

Hernacki discloses "protocol identification by heuristic content analysis." Hernacki, Title. Hernacki, however, does not teach or suggest at least "providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols independently of any predefined association between said network ports and said application layer protocols," as recited in amended claim 39 (and similarly recited in amended independent claim 57) (emphasis added). Therefore, Hernacki does not cure the deficiencies of Roesch and Yang.

Roesch, Yang, and Hernacki, therefore, whether taken alone or in combination, do not teach or suggest each and every feature of independent claims 39 and 57. Accordingly, claims

39 and 57 should be allowable over Roesch, Yang, and Hernacki. Dependent claims 48, 49, 67, and 68 should also be allowable over Roesch, Yang, and Hernacki at least by virtue of their respective dependence from base claim 39 or 57, and because they recite additional features not taught or suggested in Roesch, Yang, and Hernacki. Applicants therefore respectfully request withdrawal of the rejection.

Rejection of Claims 54, 55, 73, and 74 under 35 U.S.C. § 103(a)

Applicants respectfully traverse the rejection of claims 54, 55, 73, and 74 under 35 U.S.C. § 103(a) as being unpatentable over Roesch in view of Yang and/or Duffield. *See* Office Action, pp. 8-10.

Duffield discloses a "statistical, signature-based approach to IP traffic classification." Duffield, Title. Duffield, however, does not teach or suggest at least "providing intrusion detection on said monitored data flows based on said detected information relating to said application layer protocols independently of any predefined association between said network ports and said application layer protocols," as recited in amended claim 39 (and similarly recited in amended independent claim 57) (emphasis added). Therefore, Duffield does not cure the deficiencies of Roesch and Yang.

Roesch, Yang, and Duffield, therefore, whether taken alone or in combination, do not teach or suggest each and every feature of independent claims 39 and 57. Accordingly, claims 39 and 57 should be allowable over Roesch, Yang, and Duffield. Dependent claims 54, 55, 73, and 74 should also be allowable over Roesch, Yang, and Duffield at least by virtue of their respective dependence from base claim 39 or 57, and because they recite additional features not taught or suggested in Roesch, Yang, and Duffield. Applicants therefore respectfully request withdrawal of the rejection.

Conclusion

Applicants request reconsideration of the application and withdrawal of the objection and rejections. Pending claims 39, 41-57, and 59-77 are in condition for allowance, and Applicants request a favorable action.

The Office Action contains a number of statements reflecting characterizations of the related art and the claims. Regardless of whether any such statements are identified herein, Applicants decline to automatically subscribe to any such statements or characterizations.

Please grant any extensions of time required to enter this response and charge any additional required fees to Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: January 28, 2011

By: David M. Longo
David M. Longo
Reg. No. 53,235

/direct telephone: (571) 203-2763/